

Application Serial No. 09/844,447

1. (Currently Amended) A method for managing security information comprising the steps of:

receiving raw computer events with a fusion engine from one or more data sources, each data source comprising an intrusion detector that assigns a priority status to each raw computer event, each raw computer event comprising one of suspicious computer activity and a computer attack;

classifying the raw computer events with the fusion engine by assigning each raw computer event an event type parameter;

storing the raw computer events;

comparing each raw computer event and its type with computer environment information stored in a knowledge-based database;

assigning context parameters to each raw computer event based on the comparison of a respective computer event and its type with the computer environment information;

assigning a ranking to determining if a priority status of each raw computer event should be adjusted based on its assigned context parameters;

adjusting a priority status or leaving a priority status of a raw computer event in tact based on the determination step;

identifying one or more relationships between two or more raw computer events by using rules associated with the event type parameters and that are executed with the fusion engine by determining to determine if the two or more raw computer events are part of a larger computer attack;

in response to identifying one or more relationships between two or more raw computer events, generating a mature correlation event message; and

displaying one or more mature correlation event messages on one or more consoles that describe relationships between raw computer events.

2. (Cancelled).

Application Serial No. 09/844,447

3. (Previously Presented) The method of Claim 1, wherein the step of receiving raw computer events from one or more data sources further comprises the step of receiving real-time raw computer events from one of intrusion detection system, a detector within an intrusion detection system, and a firewall.

4. (Previously Presented) The method of Claim 1, wherein the step of receiving raw computer events from one or more data sources further comprises the step of receiving raw computer events from one of a file and database.

5. (Currently Amended) The method of Claim 1, wherein the step of classifying the raw computer events further comprises the steps of:

~~identifying an event type parameter for each raw computer event;~~  
comparing the event type parameter with an event type category of a list; and  
assigning each raw computer event to a corresponding event type category in the

list.

6. (Currently Amended) The method of Claim 1, wherein the step of ~~assigning a ranking to each raw computer event~~ assigning context parameters to each raw computer event further comprises the steps of:

comparing parameters of each raw computer event with information in a database;

and

assigning additional parameters to each raw computer event relating to the environment of the raw computer event.

7. (Original) The method of Claim 6, wherein the additional parameters comprise one of a priority status, a vulnerability status, a historical frequency value, a source zone value, a destination zone value, a detector zone value, and a text string.

Application Serial No. 09/844,447

8. (Currently Amended) The method of Claim 1, wherein the step of ~~assigning a ranking to each raw computer event~~ adjusting a priority status or leaving a priority status of a raw computer event in tact based on the determination step further comprises the steps of:

identifying a priority status parameter of a raw computer event;  
comparing each raw computer event to information contained in a ~~context database~~ knowledge-based database;

changing the priority status parameter of a respective raw computer event if a match occurs in response to the comparison step; and

leaving the priority status in tact if a match does not occur in response to the comparison step.

9. (Previous Presented) The method of Claim 1, wherein the step of identifying relationships between two or more raw computer events further comprises the steps of:

associating each raw computer event with one or more rules that correspond with a type parameter of the raw computer event; and

applying each rule to its associated group of raw computer events; and

determining if a computer attack or security breach has occurred based upon successful application of a rule.

10. (Previously Presented) The method of Claim 1, wherein the step of storing raw computer events further comprises the step of storing each raw computer event in a high speed memory device comprising random access memory (RAM).

11. (Previously Presented) The method of Claim 1, further comprising the step of determining the intent of a computer attack based upon the type of mature correlation event generated.

Application Serial No. 09/844,447

12. (Previously Presented) The method of Claim 1, further comprising the steps of:

- creating a memory management list;
- identifying a time stamp for each raw computer event; and
- adding each raw computer event to the memory management list.

13. (Previously Presented) The method of Claim 1, further comprising the step of creating a raw computer event tracking index that identifies one or more software components that are monitoring one or more raw computer events.

14. (Currently Amended) A method for determining relationships between two or more computer events, comprising the steps of:

- receiving a plurality of raw computer events with a fusion engine from one or more intrusion detectors that assign a priority parameter to each raw computer event, each raw computer event having a first set of parameters and comprising one of suspicious computer activity and a computer attack;

- creating raw computer event storage areas based upon information received from a raw computer event classification database;

- storing each event in an event storage area based upon an event type parameter;

- comparing each raw computer event to data contained in a context database with the fusion engine to determine if the two or more raw computer events are part of a larger computer attack;

- adjusting a priority parameter or leaving the priority parameter in tact for each raw computer event in response to the comparison to the context database;

- associating each raw computer event with one or more correlation events;

- applying one or more rules corresponding with the event type parameters to each raw computer event based upon the correlation event associations; and

- generating a mature correlation event message in response to each successful application of a rule.

15. (Cancelled).

Application Serial No. 09/844,447

16. (Original) The method of Claim 14, wherein the context database comprises any one of vulnerability values, computer event frequency values, source and destination zone values, and detector zone values.

17. (Original) The method of Claim 14, wherein the raw computer event classification database comprises tables that include information that categorizes raw computer events based on any one of the following: how an activity indicated by a raw computer event may impact one or more target computers, how many target computers may be affected by an activity indicated by a raw computer event, and how activities indicated by respective raw computer events gain access to one or more target computers.

18. (Currently Amended) A security management system comprising:

a plurality of data sources comprising intrusion detectors that assign a priority parameter to raw computer events;

an event collector linked to the plurality of data sources;

a fusion engine linked to the event collector, said fusion engine identifying relationships between two or more raw computer events generated by the data sources and adjusting each priority parameter if one or more conditions are met, [[by]] the fusion engine using rules associated with event type parameters assigned to each raw computer event to determining if the two or more raw computer events are part of a larger computer attack, each raw computer event comprising one of suspicious computer activity and a computer attack; and

a console linked to the event collector for displaying any output generated by the fusion engine.

19. (Previously Presented) The security management system of Claim 18, wherein each intrusion detector runs in a kernel mode of a computer and the fusion engine runs in a user mode of the computer.

Application Serial No. 09/844,447

20. (Previously Presented) The security management system of Claim 18, wherein each intrusion detector comprises a chip, and the fusion engine comprises software running on a computer.

21. (Previously Presented) The security management system of Claim 18, wherein each intrusion detector comprises a board, and the fusion engine comprises software running on a computer.

22. (Currently Amended) A fusion engine comprising:

a controller;

an event reader for receiving raw computer events from intrusion detectors that assign a priority parameter to each raw computer event, each raw computer event comprising one of suspicious computer activity and a computer attack;

a classifier linked to the event reader for classifying the received raw computer events;

a raw computer event classification database linked to the classifier;

a context based risk-adjustment processor linked to the classifier, for adjusting priorities the priority parameters of raw computer events;

a context database linked to the context based risk-adjustment processor for providing context parameters that are assigned to raw computer events and that are used by the context based risk-adjustment processor; and

a rule database[[.]] that comprises rules for identifying if one or more relationships exist between two or more events by determining if the two or more raw computer events are part of a larger computer attack.

23. (Previously Presented) The fusion engine of Claim 22, further comprising an event reporter, a mature event list, a memory management list, and a raw computer event tracking index .

Application Serial No. 09/844,447

24. (Original) The fusion engine of Claim 22, wherein the context database comprises any one of vulnerability values, computer event frequency values, source and destination zone values, and detector zone values.

25. (Previously Presented) The fusion engine of Claim 22, wherein the raw computer event classification database comprises tables that include information that categorizes raw computer events based on any one of the following: how an activity indicated by a raw computer event may impact one or more target computers, how many target computers may be affected by an activity indicated by a raw computer event, and how activities indicated by respective raw computer events gain access to one or more target computers.

26. (Currently Amended) A method for managing security information comprising the steps of:

receiving with a fusion engine a raw computer event having a first ranking from one or more data sources comprising intrusion detectors, each raw computer event comprising one of suspicious computer activity and a computer attack;

classifying the raw computer event with the fusion engine by assigning each raw computer event an event type parameter;

storing the raw computer event; [[and]]

assigning a second ranking to the raw computer event with the fusion engine, ~~whereby~~ the second ranking assesses risks of the raw computer event based upon a context of the raw computer event ~~and indicates;~~

determining if the first ranking each raw computer event should be adjusted based on its second ranking; and

identifying one or more relationships between two or more raw computer events by using rules associated with event type parameters to determine if the raw computer event is part of a larger computer attack.

27. (Previously Presented) The method of Claim 26, wherein the first ranking comprises one or more relative values measuring potential risk or damage that is associated with the raw computer event.

Application Serial No. 09/844,447

28. (Previously Presented) The method of Claim 26, wherein the step of assigning a second ranking to each raw computer event further comprises the steps of:

- comparing parameters of each raw computer event with information in a database;
- and
- assigning additional parameters to each raw computer event relating to the environment of the raw computer event.

29. (Previously Presented) The method of Claim 28, wherein the additional parameters comprise at least one of a priority status, a vulnerability status, a historical frequency value, a source zone value, a destination zone value, a detector zone value, and a text string.

30. (Currently Amended) The method of Claim 26, wherein the first ranking comprises a priority status parameter, and the step of determining if the first ranking of each raw computer event should be adjusted based on its second ranking further comprises step of assigning a second ranking to each raw computer event further comprises the steps of:

- ~~identifying a priority status parameter of a raw computer event;~~
- comparing the second ranking of each raw computer event to information contained in a context database;
- changing the priority status parameter of a respective raw computer event if a match occurs in response to the comparison step; and
- leaving the priority status in tact if a match does not occur in response to the comparison step.

[The remainder of this page has been intentionally left blank.]



Application Serial No. 09/844,447

31. (Currently Amended) A method for managing security information comprising the steps of:

receiving raw computer events with a fusion engine from one or more data sources comprising intrusion detectors that assign a priority status to each raw computer event, each raw computer event comprising one of suspicious computer activity and a computer attack;

classifying the raw computer events with the fusion engine by assigning each raw computer event an event type parameter;

assigning context parameters to each raw computer event based on the comparison of a respective computer event and its type parameter with computer environment information;

determining if a priority status of each raw computer event should be adjusted based on its context parameters;

grouping two or more raw computer events into a high level correlation event with the fusion engine if the two or more raw computer events are part of a larger computer attack;

in response to grouping the two or more raw computer events, applying one or more rules to the raw computer events;

generating a mature correlation event message if application of a rule is successful; and

displaying one or more mature correlation event messages on a console that describe relationships between raw computer events, ~~whereby a number of event displayed on the console are substantially minimized.~~

32. (Cancelled).

33 (Previously Presented) The method of Claim 31, wherein the step of receiving raw computer events from one or more data sources further comprises the step of receiving real-time raw computer events from one of intrusion detection system, a detector within an intrusion detection system, and a firewall.

Application Serial No. 09/844,447

34. (Previously Presented) The method of Claim 31, wherein the step of receiving raw computer events from one or more data sources further comprises the step of receiving raw computer events from one of a file and database.

35. (Cancelled).

36. (Previously Presented) The method of Claim 31, wherein the step of classifying comprises the step of categorizing a raw computer event based on any one of the following: how a raw computer event may impact one or more target computers, how many target computers that may be affected by a raw computer event, and how respective raw computer events gain access to one or more target computers.

37. (Previously Presented) The method of Claim 31, wherein the step of grouping two or more raw computer events further comprises the step of determining a time at which a respective raw computer event occurred relative to another raw computer event.

38. (Previously Presented) A computer readable medium having computer-executable instructions for performing the steps recited in Claim 1.

39. (Previously Presented) A computer readable medium having computer-executable instructions for performing the steps recited in Claim 14.

40. (Previously Presented) A computer readable medium having computer-executable instructions for performing the steps recited in Claim 26.

41. (Previously Presented) A computer readable medium having computer-executable instructions for performing the steps recited in Claim 31.

[The remainder of this page has been intentionally left blank.]